Practical remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem

S. Wu [*]

Abstract

Most recently, Yang et al proposed an ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem in journal of Computer and Security. In this paper, we find some disadvantages in their scheme and thereafter propose such an improved scheme that overcomes all those disadvantages existing in their scheme while the merits are left unchanged. Our scheme provides more guarantees in security as follows: (1) our scheme combines two factors to protect its authentication mechanism. (2) our scheme can safely provide mutual authentication and key agreement with more desirable properties. (3) our scheme can provide anonymity for the user's identity. And yet, our scheme is simpler and more efficient than Yang et al's scheme. Therefore the end result is more practical for the users of mobile devices.

Key words: ID-based; mutual authentication; key agreement; anonymity; mobile device.

1 Introduction

With the advancement and tremendous development of wireless technology, various mobile devices has prevailed in our daily life, e.g. cell phone, PDA, and so on. By the mobile devices, people can accomplish the electronic transactions anytime and anywhere. Thus, more and more electronic transactions for mobile devices are implemented on Internet or wireless networks. In this paper, we study remote authentication scheme especially for efficient implementation on wireless mobile devices. Since the computation ability and battery capacity of mobile devices are limited, the natural choice would be elliptic curve (EC)

[*] Corresponding author.
Email address: pqwsh@yahoo.com.cn (S. Wu).

based authentication schemes because of the well-known advantages with regard to processing and size constraints[1,2].

Recently, various authentication schemes based on elliptic curve are proposed [3–11]. As noted in [12], most schemes on elliptic curve cryptosystem (ECC) accomplished authentication using public-key and thus needed a key authentication center (KAC) to maintain the certificates for users' public keys. In addition, users often needs to perform additional computations to verify the certificate in these schemes(e.g. [3,6–10]). This causes the computation loads and the energy costs of mobile devices very high. To solve the above problems, several ID-based authentication schemes on ECC are proposed, e.g. [4,5,11]. In an ID-based scheme, the user utilizes his unique identity (e.g., name, address, or email address) as his public key. However, these ID-based authentication schemes on ECC[4,11] are constructed by using bilinear pairings, which is an expensive operation [5]. For mobile devices, the computation and energy costs of the pairing-based schemes are higher than those of of EC-based schemes without pairing.

Most recently, Yang et al [12] proposed such an ID-based remote mutual authentication with key agreement scheme on ECC that does not require the costly bilinear-pairing operations. Although, their scheme is superior the previous solutions for implementation on mobile devices, we still find some disadvantages in their scheme:

(1) The authentication mechanism in their scheme depends solely on a long-term private key stored in the mobile device(or the card), which is risky because one can easily impersonate the user if he gets the device(this assumption is reasonable because the users may lose his mobile device sometimes).

(2) If the user's long-term key is compromised(this assumption is also reasonable because the users may be careless or unskilled at protecting their private keys), the adversary will not only be able to masquerade as the user but also as the server. The latter case is even worse because the adversary may impersonate a service provider to fool the victims into revealing more secret information about them. Moreover, the adversary can reveal all the previous session keys of that user.

(3) Their scheme does not consider personal privacy problem since the user's identity is sent in plain over the open network. Today, many people give great concerns on their personal privacy problem and prefer a secure authentication protocol with anonymity to protect some sensitive information about them. These sensitive information could be a buyer's movement, individual's social circle, shopping patterns and individual preferences etc [13]. However, Yang et al's scheme do not address the problem.

These disadvantages make their authentication scheme on ECC unsuitable for some critical applications like electronic commerce.

In this, we present such an improved scheme that overcomes those disadvantages existing in Yang et al's scheme while the merits of their scheme are left unchanged. Our scheme provides more guarantees in security as follows:

(1) Firstly, our scheme is a two-factor mutual authentication scheme based on smart cards and passwords so that one must have the smart-card and know the password in order to gain access to the server.
(2) Secondly, our scheme can safely provide mutual authentication with key agreement phase between the user and the server. Even in an extreme case that the user's long-term private key is compromised, the intruder can not impersonate the server to the user. Furthermore, the attacker can not know any information about those previously established session keys even when the server's key is compromised too.
(3) Thirdly, our scheme can provide anonymity for the user's identity.

Furthermore, our scheme is simpler than more efficient than Yang et al's scheme in [12]. Therefore, the end result is more suited to be a candidate for implementation on mobile devices.

The remainder of this paper is organized as follows. Section 2 reviews Yang et al's scheme briefly and then points out the disadvantages existing in their scheme. Section 3 provides an improved scheme to overcome all those disadvantages existing in their scheme. In addition, some important discussions are also made in this section. Finally, conclusion is presented in Section 4.

2 Review of Yang et al's Scheme

In this section, we briefly review Yang et al's scheme in [12]. Their scheme provides the mutual authentication and a session key agreement between a user U and a remote server S. It is divided into two phases: user registration phase and mutual authentication with key agreement phase. First, we define some notations used in Yang et al's scheme in Table 1.

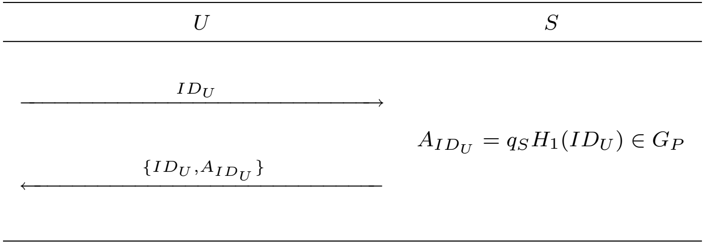
Now, we introduce Yang et al's scheme. And a detailed description of the scheme follows. Here, we just follow the description in [12].

Registration phase: U must register to S to become a legal user as follows, which is described in Fig 1.

Table 1. The notations used in Yang et al's scheme

ID_U	the identity of the user U
$\mathcal{E}$	an elliptic curve defined over a prime finite field $\mathbb{F}_p$ with large order
P	a base point in $\mathcal{E}$ with large order q, where q is a secure large prime
G_P	a cyclic addition group generated by P
$x \cdot P$	the point multiplication defined as $x \cdot P = \underbrace{P + P + \cdots + P}_{x\ times}$
(q_S, Q_S)	the server S's private/public key pair, where $Q_S = q_S \cdot P$
$H_1(\cdot)$	a secure one-way hash function: $\{0,1\}^* \rightarrow G_P$
$H_2(\cdot)$, $H_3(\cdot)$	two secure one-way hash functions: $\{0,1\}^* \rightarrow Z_p^*$

Fig. 1. Registration phase of Yang et al's scheme.



Step 1. The user U sends his identity ID_U to the server.

Step 2. The server S computes $A_{ID_U} = q_S H_1(ID_U) \in G_P$, where A_{ID_U} is the authentication key for the user U. Then, S sends A_{ID_U} to U in a secure channel.

Step 3. After receiving A_{ID_U} , U checks if A_{ID_U} is valid. If it is valid, U keeps A_{ID_U} in private.

Mutual authentication with key agreement phase: U and S authenticate each other and negotiate the common session key for later communications. The detailed steps are described as follows and the handshake between U and S is depicted in Fig 2.

Step 1. The user U randomly chooses a point $R_U = (x_U, y_U)$in $\mathcal{E}$, where x_U and y_U are x and y coordinates of point R_U, respectively. Then, U computes $t_1 = H_2(T_1)$, $M_U = R_U + t_1 \cdot A_{ID_U}$ and $\overline{R}_U = x_U \cdot P$, where T_1 is a timestamp denotes the current time. Finally, U sends $(ID_U, M_U, \overline{R}_U, T_1)$ to the server.

Step 2. After receiving $(ID_U, M_U, \overline{R}_U, T_1)$, the server S computes $Q_{ID_U} = H_1(ID_U)$, $t_1 = H_2(T_1)$ and $R_U^{'} = M_U - q_S \cdot t_1 \cdot Q_{ID_U}$ to obtain $Q_{ID_U} = (x_Q, y_Q)$ and $R_U^{'} = (x_U^{'}, y_U^{'})$. Then, S checks if $\overline{R}_U = x_U^{'} \cdot P$ holds. If the equation holds, the server confirms that U is valid and $x_U^{'} = x_U$. Otherwise, the protocol is terminated.

Step 3. The server S randomly chooses a point $R_S = (x_S, y_S)$in $\mathcal{E}$, and then

Fig. 2. Mutual authentication with key agreement phase of Yang et al's scheme.

User U		Server S
$R_U = (x_U, y_U) \in \mathcal{E}$		
$t_1 = H_2(T_1) \in Z_p^*$		
$M_U = R_U + t_1 \cdot A_{ID_U}$		
$\overline{R}_U = x_U \cdot P$	$\xrightarrow{(ID_U, M_U, \overline{R}_U, T_1)}$	$Q_{ID_U} = H_1(ID_U) = (x_Q, y_Q)$
		$t_1 = H_2(T_1)$
		$R_U^{'} = M_U - q_S \cdot t_1 \cdot Q_{ID_U} = (x_U^{'}, y_U^{'})$
		$\overline{R}_U \stackrel{?}{=} x_U^{'} \cdot P$
		$R_S = (x_S, y_S) \in \mathcal{E}$
		$t_2 = H_2(T_2) \in Z_p^*$
		$M_S = R_S + t_2 \cdot q_s \cdot Q_{ID_U}$
		$k = H_3(x_Q, x_U, x_S)$
$Q_{ID_U} = H_1(ID_U) = (x_Q, y_Q)$	$\xleftarrow{(M_S, M_k, T_2)}$	$M_k = (k + x_S) \cdot P$
$t_2 = H_2(T_2) \in Z_p^*$		
$R_S^{'} = M_S - t_2 \cdot A_{ID_U} = (x_S^{'}, y_S^{'})$		
$k^{'} = H_3(x_Q, x_U, x_S^{'})$		
$M_k \stackrel{?}{=} (k^{'} + x_S^{'}) \cdot P$		

it computes $t_2 = H_2(T_2)$ and $M_S = R_S + t_2 \cdot q_s \cdot Q_{ID_U}$. Then, S computes the session key k by the equation $k = H_3(x_Q, x_U, x_S)$. Finally, S computes $M_k = (k + x_S) \cdot P$ and sends (M_S, M_k, T_2) to U.

Step 4. After receiving (M_S, M_k, T_2), the user U computes $Q_{ID_U} = H_1(ID_U)$, $t_2 = H_2(T_2)$, and $R_S^{'} = M_S - t_2 \cdot A_{ID_U}$ to derive $Q_{ID_U} = (x_Q, y_Q)$ and $R_U^{'} = (x_S^{'}, y_S^{'})$. Then, U computes the equations $k^{'} = H_3(x_Q, x_U, x_S^{'})$ and $M_k^{'} = (k^{'} + x_S^{'}) \cdot P$ to check if $M_k^{'} = M_k$ holds. If the equation holds, U can confirm that S is valid and the session key $k^{'}$ is equal to k. Otherwise, the protocol is terminated.

According to Yang et al.'s scheme [12], we find that the ID-based remote authentication scheme on ECC has the following disadvantages. First, the authentication mechanism in their scheme depends solely on a long-term private key A_{ID_U}, which can be risky because an attacker can successfully forge U to communicate with S if the card used to store this key is stolen by the attacker. Second, when the user's long-term key is compromised, the adversary will not only be able to masquerade as the user but also as the server. Usually, when the long-term key of a user is compromised, the adversary will be able to masquerade as the user but the situation will be even worse if the adversary can also masquerade as the server because the adversary can impersonate a service provider to fool the victims into revealing more secret information about them. Moreover, the adversary can reveal all the previous session keys of that user. Third, their scheme does not consider personal privacy problem since the user's identity is sent in plain over the open network. In the past decade, there are many researches that point out some behaviors such as the information of the customer behavior and track of the user are the personal privacy. Thus, the behavior of users should be done anonymous. These disadvantages make their authentication schemes on ECC unsuitable for some electronic transactions. Fourth, their scheme lacks formal security proof. To overcome these disadvantages, we propose an improved ID-based remote mutual authentication scheme on ECC with anonymity for mobile devices in the next section.

3 Our Improved Protocol

In this section, we present an improved scheme to overcome those disadvantages existing in Yang et al's scheme[12] while the merits of the original scheme are left unchanged. Finally, we also provide some important remarks on it in this section.

3.1 Description

This subsection describes our improved protocol, starting with some definitions and notations used in our scheme.

First, we introduce the new notations different from those listed in Table 1 as follows: $H_1(\cdot)$, $H_2(\cdot)$ and $H_3(\cdot)$ are now defined as three secure one-way hash functions : $\{0,1\}^* \rightarrow Z_q^*$ instead, where l is the security parameter. In addition to (q_S, Q_S), the server also has a private key d_S. The security of our protocol mainly relies on the EC computational Diffie-Hellman (ECCDH) assumption. In the ECCDH assumption, given $W = w \cdot P$ and $V = v \cdot P$, where w and v are drawn randomly from Z_q^*, it is computationally infeasible to compute $uv \cdot P$(denoted by $ECCDH(W, V)$). The rest of notations are referred to Table 1.

Now, we introduce our improved scheme. Like Yang et al's scheme, our scheme also consists of two phases: user registration phase and mutual authentication with key agreement phase. However, we combine two factors authentication mechanisms in our scheme so that one must have the smart-card and know the password in order to gain access to the server. That is, our scheme is smart-card-based password authentication scheme. Furthermore, we send the user's shadow identity instead in the open network so that anonymity is achieved in our improved scheme. A more detailed description follows:

Registration phase: Server S issues a smart-card to user U as follows, which is described in Fig 3.

Fig. 3. Registration phase of our scheme.

U	S
$\xrightarrow{ID_U}$	
	$B_U = A_{ID_U} \oplus H_2(PW_0) = H_1(ID_U, d_S) \oplus H_2(PW_0)$
$\xleftarrow{\{ID_U, B_U\}}$	

Step 1. The user U sends his identity ID_U to the server.

Step 2. The server S computes $A_{ID_U} = H_1(ID_U, d_S)$ and then $B_U = A_{ID_U} \oplus H_2(PW_0)$, where $\oplus$ is the exclusive-OR operation on bit strings and PW_0 the initial password (e.g. a default password such as a string of all "1"). Then, S issues U a smart-card which contains ID_U, B_U and all the system parameters needed in our scheme.

Step 3. After receiving the smart-card , U changes the password immediately.

Mutual authentication with key agreement phase: U inserts his smart card into the mobile input device and enters password PW_U. The smart-card retrieves the value $A_{ID_U} = B_U \oplus H_2(PW_U)$. U (actually performed by the user's smart-card) and S then use A_{ID_U} to perform the protocol as follows, which is described in Fig 4.

Fig. 4. Mutual authentication with key agreement phase of our scheme.

User U		Server S
$A_{ID_U} = B_U \oplus H_2(PW_U)$		
$x \xleftarrow{R} Z_q^*; X = x \cdot P, T = x \cdot Q_S$		
$SID = ID_U \oplus H_3(\text{"0"}, X, Q_S, T)$		
$\alpha = H_3(\text{"1"}, X, SID, A_{ID_U})$	$\xrightarrow{(X, SID, \alpha)}$	$T = q_S \cdot X$
		$ID_U = SID \oplus H_3(\text{"0"}, X, Q_S, T)$
		$A_{ID_U} = H_1(ID_U, d_S)$
		$\alpha' = H_3(\text{"1"}, X, SID, A_{ID_U})$
		$\alpha' \overset{?}{=} \alpha$
		$y \xleftarrow{R} Z_q^*; Y = y \cdot P, Z = y \cdot X$
$Z = x \cdot Y$	$\xleftarrow{(Y, \beta)}$	$\beta = H_3(\text{"2"}, X, Y, SID, Z, T, A_{ID_U})$
$\beta' = H_3(\text{"2"}, X, Y, SID, Z, T, A_{ID_U})$		
$\beta' \overset{?}{=} \beta$		
$\gamma = H_3(\text{"3"}, X, Y, SID, Z, T, A_{ID_U})$	$\xrightarrow{(\gamma)}$	$\gamma' = H_3(\text{"3"}, X, Y, SID, Z, T, A_{ID_U})$
		$\gamma' \overset{?}{=} \gamma$
$k = H_3(\text{"4"}, X, Y, SID, Z, T, A_{ID_U})$		$k = H_3(\text{"4"}, X, Y, SID, X, T, A_{ID_U})$

Step 1. The user U first chooses a random number $x \in Z_q^*$ and computes $X = x \cdot P$ and $T = x \cdot Q_S$. Then he generates the shadow identity $SID = ID_U \oplus H_3(\text{"0"}, X, Q_S, T)$ and the authenticator $\alpha = H_3(\text{"1"}, X, SID, A_{ID_U})$. Finally, he sends (X, SID, α) to the server S.

Step 2. After receiving (X, SID, α), the server S first computes $T = q_S \cdot X$ and obtains $ID_U = SID \oplus H_3(\text{“0”}, X, Q_S, T)$. Then he computes $A_{ID_U} = H_1(ID_U, d_S)$ and $\alpha' = H_3(\text{“1”}, X, SID, A_{ID_U})$, and checks if $\alpha = \alpha'$ holds. If the equation doest not hold, the protocol is terminated. Otherwise, the server confirms that the received message is generated by the valid user U. Finally, the server S authenticate itself to the user U. More specifically, he chooses a random number $y \in Z_p^*$, computes $Y = y \cdot P$, $Z = y \cdot X$ and $\beta = H_3(\text{“2”}, X, Y, SID, Z, T, A_{ID_U})$, and sends (Y, β) to the user U.

Step 3. After receiving (Y, β), the user U computes $Z = x \cdot Y$ and $\beta' = H_3(\text{“2”}, X, Y, SID, Z, T, A_{ID_U})$. Then he checks if $\beta = \beta'$ holds. If the equation doest not hold, the protocol is terminated. Otherwise, the server confirms that the responder is the valid server S. Then he authenticate itself to S by computing $\gamma = H_3(\text{“3”}, X, Y, SID, Z, T, A_{ID_U})$ and sending the authenticator γ to S. Finally, he computes the session key $k = H_3(\text{“4”}, X, Y, SID, Z, T, A_{ID_U})$ and accepts and terminates the session.

Step 4. After receiving (γ), the server S computes $\gamma' = H_3(\text{“3”}, X, Y, SID, Z, T, A_{ID_U})$ to check if $\gamma' = \gamma$ holds. If the equation holds, U can confirm that the initiator is the valid user U. Finally, he computes the session key $k = H_3(\text{“4”}, X, Y, SID, X, T, A_{ID_U})$ and accepts and terminates the session.

The correctness of our protocol follows from the fact that, in an honest execution of the protocol, $T = x \cdot Q_S = q_S \cdot X$ and $Z = x \cdot Y = y \cdot X$.

3.2 Discussions

In this subsection, we discuss its attractive features in contrast to Yang et al's scheme. To the best of our knowledge, Yang et al's scheme[12] is superior to previously proposed schemes [3–11]. For this reason, we only compare the proposed scheme with their scheme.

Our scheme provides more guarantees in security[1] as follows:

(1) Our scheme is a two-factor mutual authentication scheme based on smart cards and passwords. At the protocol level, A_{ID_U} is indeed the authentication data used in the mutual authentication phase. Therefore, in order to gain access to the server, one must have the smart-card and know the password of the user so that the value A_{ID_U} can be retrieved to perform the protocol. Even in an extreme case that the adversary gets the user's smart cart, our scheme still can protect the password information

[1] We can provide the rigorous proof of the security for our scheme under the assumptions that the hash function closely behaves like a random oracle and that the EC computational Diffie-Hellman problem is difficult. The security model is that Bellare, and Rogaway [14] for the password case. We omitted here

against the notorious password guessing attacks by which attackers could search the relatively small space of human-memorable passwords. Without knowing the password, he can not gain the service from the server yet.

(2) Our scheme can safely provide mutual authentication with key agreement between the user and the server:

- Firstly, provided that the authentication data A_{ID_U} is not compromised, the adversary can not successfully impersonate the user to send a valid authenticator γ for the challenge Y or impersonate the server to rely with a valid authenticator β for the challenge X. At the same time, the adversary can retrieve no information about the session, which is derived from the secret value A_{ID_U} and the fresh challenges(can be seen as nonces). We should note that the last round of the communication in Fig 4 is necessary since the server can only confirm the first message (X, SID, α) is generated by U by checking validness of α. However, this message could be the replayed message generated in some previous execution. Only when the user sends a valid γ for the challenge Y, the server can confirm the initiator is valid, where Y can be regarded as the nonce of the server.
- Secondly, we consider an extreme case that the user's long-term private key A_{ID_U} is compromised. Although the intruder can impersonate the user to the server, he can not impersonate the server to rely with a valid authenticator β to the user for the challenge X or obtains the current session key of the user since he can not know the value of $T = ECCDH(X, Q_S)$ based on the hardness of elliptic curve computational Diffie-Hellman problem.
- Thirdly, even when both the user's the long-term keys and the server's keys are compromised, the adversary can not know the previous session keys that were established before the corruption (which is usually called forward secrecy).

(3) Our scheme can provide anonymity for the user's identity. Here, we assume that the authentication data A_{ID_U} is not compromised. Upon receiving the message (X, SID, α), the server accepts this message only when he confirms it is generated by U after checking the value of α is valid. As a result, the adversary can not obtains the user's identity from SID since he can not know the value of $T = ECCDH(X, Q_S)$ with X generated by U based on the hardness of elliptic curve computational Diffie-Hellman problem.

To sum up, our scheme overcomes all disadvantages in security mentioned in the section 3.

On the other hand, the merits of Yang et al's original scheme in [12] are left unchanged in the our scheme:

- Firstly, like Yang et al's original scheme, our scheme also utilizes user's unique identity ID_U to compute A_{ID_U} for mutual authentication, instead of using public keys. Due to it, the users and the server do not need to perform additional computations for verifying the other party's certificates, which provides efficiency for the users of mobile devices; and on the other hand, the server does not need to maintain a large public-key table while the number of users becomes very large, which provides high scalability for the user addition in electronic transactions.
- Secondly, our scheme also requires no pairing computations but only point-multiplication operations on elliptic curve. Compared with the pairing-based authentication schemes [4,8,9,11], the proposed scheme has less computation loads for mobile devices since pairing computation is much more expensive than point-multiplication operation on ECC [5].
- Thirdly, our scheme also provides the mutual authentication between the user and the server. Over some previous remote user authentication schemes on ECC[6–8,11] that only allow the server to authenticate the validity of the users' identities, our scheme also has such an advantage: no attacker can impersonate the sever to steal the user's secret information any more.
- Fourthly, like Yang et al's original scheme[12], our scheme not only accomplishes the mutual authentication but also provides a session key agreement between a user and the remote server. Thus, the proposed scheme is flexible for many applications. However, some of the previous authentication schemes on ECC[5,8,11] can be only implemented to the remote login system because they only provide the user authentication without a session key agreement for users and a remote server.

Furthermore, our scheme is simpler and more efficient than Yang et al's scheme in[12].

- Firstly, we use nonces instead of timestamps to avoid the clock synchronization problem. Although one more round of communication is needed, an additional clock synchronization mechanism is not needed. Note X and Y could be seen as the nonce of the user and the server respectively in our scheme.
- Secondly, the validness of each message received can be checked efficiently. Since each message is sent along with a hashing value as its authenticator in our scheme, both the user and the server needs to perform a hashing operation and then make comparison in a straightway to validate a message. However, to achieve the same goal, each party needs to perform two point multiplication plus a point addition operations in Yang et al's scheme. A hashing computation can be done much more efficiently both in time and energy consumption than point operations, based on the experimental results of related researches[15–20]. As a result, a lot of operating time and energy used in checking could be saved if an invalid message is received. Therefore, our scheme is more robust.

- Thirdly, our scheme is computationally efficient than Yang et al's scheme. As shown in Table 2, on one honest run of our authentication protocol, each party needs to perform one less point multiplication and two point additions.
- Besides, our scheme allows mobile uses to change their password freely.

Finally, we list the comparisons of our scheme and Yang et al's scheme on ECC in Table 2. Based on the results listed in the table, we conclude that our scheme is more practical than the related schemes for the users of mobile devices.

Table 2. Comparisons with Yang et al's work

Properties		Schemes	
		Yang et al	Ours
security	authentication mechanism	one-factor	two-factor
	A_{ID_U} compromised impersonation	U and S	U
	anonymity	No	Yes
performance	Computation costs *	4PM+2PA	3PM
	Communication rounds	2	3

*PM: Elliptic curve point multiplication; PA: Elliptic curve point addition.

4 Conclusion

In this paper, we have proposed such an improved scheme that overcomes those disadvantages existing in Yang et al's scheme while the merits of the their scheme are left unchanged. Our scheme can provide more guarantees in security with several desirable properties. And yet, our scheme is simpler and more efficient than Yang et al's scheme in [12]. Therefore, our scheme is more practical than the previous related schemes for the users of mobile devices.

References

[1] D. Hankerson, A. Menezes, S. Vanstone. Guide to elliptic curve cryptography. Springer-Verlag, New York, USA, 2004.

[2] N. Koblitz. Elliptic curve cryptosystem. Mathematics of Computation, 1987, 48, 203-209.

[3] Abichar PE, Mhamed A, Elhassan B. A fast and secure elliptic curve based authenticated key agreement protocol for low power mobile communications.

In: Proceedings of the 2007 international conference on next generation mobile applications, services and technologies; 2007. p. 235-40.

[4] Choie YJ, Jeong E, Lee E. Efficient identity-based authenticated key agreement protocol from pairings. Applied Mathematics and Computation 2005;162:179C88.

[5] Cao X, Kou W, Dang L, Zhao B. IMBAS: identity-based multi-user broadcast authentication in wireless sensor networks. Computer Communications 2008;31:659C67.

[6] Chen ZG, Song XX. A distributed electronic authentication scheme based on elliptic curve. In: Proceedings of the sixth international on machine learning and cybernetics; 2007. p. 2179C182.

[7] Jiang C, Li B, Xu H. An efficient scheme for user authentication in wireless sensor networks. In: Proceedings of 21st international conference on advanced information networking and applications workshops; 2007. p. 438C42.

[8] Jia Z, Zhang Y, Shao H, Lin Y, Wang J. A remote user authentication scheme using bilinear pairings and ECC. In: Proceedings of the sixth international conference on intelligent system design and applications; 2006. p. 1091C94.

[9] Liao YP, Wang SS. A secure and efficient scheme of remote user authentication based on bilinear pairings. In: Proceedings of 2007 IEEE region 10 conference; 2007. p. 1C4.

[10] Tian X, Wong DS, Zhu RW. Analysis and improvement of authenticated key exchange protocol for sensor networks. IEEE Communications Letters 2005;9(11):970C2.

[11] Wu ST, Chiu JH, Chieu BC. ID-based remote authentication with smart cards on open distributed system from elliptic curve cryptography. In: Proceedings of IEEE international conference on electro information technology; 2005.

[12] J.-H.o Yang, C.-C. Chang. An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem, computers and security, 28(2009): 138-143.

[13] C.-H Yun, M.-S. Chen, Ming mobile sequential patterns in a mobiel commerce environment, IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews 37(2)(2007) 278-295.

[14] Mihir Bellare and Phillip Rogaway. Provably secure session key distribution — the three party case. In 28th Annual ACM Symposium on Theory of Computing, pages 57-66, Philadephia, Pennsylvania, USA, May 22-24, 1996. ACM Press.

[15] D.S. Wong, H.H. Fuentes, A.H. Chan, The performance measurement of cryptographic primitives on palm devices, in: Proceedings of the 17th Annual Computer Security Applications Conference (ACSAC 2001), New Orleans, USA, 2001, pp. 92-101.

[16] P.G. Argyroudis, R. Verma, H. Tewari, D. OMahony, Performance analysis of cryptographic protocols on handheld devices, in: Proceedings of the 3rd IEEE International Symposium on Network Computing and Applications (NCA 2004), Cambridge, USA, Sep. 2004, pp. 169-174.

[17] M. Passing, F. Dressler, Experimental performance evaluation of cryptographic algorithms, in: Proceedings of the 3rd IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS), Vancouver, Canada, 2006, pp. 882-887.

[18] M. Passing, F. Dressler, Practical evaluation of the performance impact of security mechanisms in sensor networks, in: Proceedings of the 31st IEEE Conference on Local Computer Networks, Tampa, USA, 2006, pp. 623-629.

[19] M.R. Doomun, K.S. Soyjaudah, D. Bundhoo, Energy consumption and computational analysis of Rijndael-AES, in: Proceedings of the Third IEEE International Conference in Central Asia on Internet the Next Generation of Mobile, Wireless and Optical Communications Networks (ICI 2007), Uzbekistan, 2007, pp. 1-6.

[20] N.R. Potlapally, S. Ravi, A. Raghunathan, N.K. Jha, A study of the energy consumption characteristics of cryptographic algorithms and security protocols, IEEE Transactions on Mobile Computing 5 (2) (2006) 128-143.